MULTINATIONAL EXPERIMENT 7

CATALOG OF PRODUCTS

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
08 JUL 2013	**Final**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
MNE 7 Product Catalogue	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Joint Staff J7 - MN/ACT Integration 116 Lakeview Parkway Suffolk, VA 23435**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT
The products outlined in this catalog represent the final outcomes generated during this seventh MNE campaign, Access to the Global Commons. MNE 7 was a complex, two-year, multinational and inter-agency effort designed to improve coalition capabilities relative to ensuring access to the global commons. MNE 7 had 18 participating nations and organizations and proved to be the most ambitious campaign to date.

15. SUBJECT TERMS
MNE 7, Multinational, Experiment Catalogue, Access, Global, Commons, Maritime, Security, Space, Cyber, Inter-Domain, Synthesis

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**36**	

From the Chair of the Executive Steering Group

The Multinational Experiment (MNE) Program commenced in 2001 and initially involved four participating nations. During the past 11 years, the MNE series has progressed and expanded to encompass seven campaigns where the collaborative work has produced outcomes that benefited 22 nations and international organizations. The MNE Program has proven to be a cost effective means for all participating nations to find viable solutions to existing and future capability gaps.

The products outlined in this catalog represent the final outcomes generated during this seventh MNE campaign, "Access to the Global Commons." MNE 7 was a complex, two-year, multinational and inter-agency effort designed to improve coalition capabilities relative to ensuring access to the global commons. MNE 7 had 18 participating nations and organizations and proved to be the most ambitious campaign to date.

MNE 7 outcomes have the potential to significantly enhance both coalition and national operating capabilities while narrowing known gaps. This latest campaign has served to increase collective understanding within each of the separate domains and provided the opportunity to further explore the nature of their interconnectedness. MNE 7 products provide a common foundation for change recommendations in the areas of doctrine, organization, training, materiel, leadership education, personnel, facilities, and policy.

It is great news to hear that some of these outcomes are already being transitioned toward implementation.

To obtain a copy of a product listed in the catalog, please send a request to the MNE 7 Secretariat, mne7_secretariat@apan.org.

Sincerely,

Brian D. Beaudreault
Brigadier General, US Marine Corps
Chair, MNE Executive Steering Group

THIS PAGE INTENTIONALLY LEFT BLANK.

Table of Contents

MULTINATIONAL EXPERIMENT 7

Access to the Global Commons

The Multinational Experiment (MNE) series was initiated by United States Joint Forces Command (USJFCOM) in 2001 and is now led by Joint and Coalition Warfighting, Joint Development, United States Joint Staff J7. It is designed to develop and validate concepts and capabilities that can be used to address the challenges associated with conducting coalition operations. To date, six experimentation campaigns have been conducted in this series. For the current seventh campaign, the two-star level MNE Executive Steering Group decided to focus on the critical problem of ensuring access to the global commons.

MNE 7 Problem Statement

Nations and organizations require concepts and capabilities for anticipating, deterring, preventing, protecting against and responding to a disruption or a denial of access to the global commons domains (air, maritime, space and cyber) and for ensuring freedom of action within them, while taking into account their interrelationships.

MNE 7 is a two-year multinational and interagency effort designed to improve coalition capabilities to ensure access to and use of the global commons domains through application of the comprehensive approach. The nations and organizations currently participating in MNE 7 are Austria, Canada, Denmark, the European Union Military Staff (Observer), Finland, France, Germany, Hungary, Italy, the North Atlantic Treaty Organization (NATO) Allied Command Transformation (ACT), Netherlands (Observer), Norway, Poland, the Republic of Korea, Spain, Sweden, Switzerland, Turkey (Observer), the United Kingdom, and the United States.

WHY ARE THE GLOBAL COMMONS IMPORTANT?

Access to the global commons is clearly vital in maintaining the capability to conduct expeditionary military operations. This, however, is only the beginning. Massive quantities of goods, people and information flow through the global commons every day. For example, ninety percent of all global trade is conducted by sea. Over two billion passengers travel by air each year. Outer space is used to enable communications, imagery and navigation by civil, military and commercial actors. Financial transactions worth several trillion dollars are conducted via cyberspace every day. Thus, access to and freedom of action with the global commons is far more than a military necessity. It is an essential prerequisite for the daily business of modern life.

MNE 7 uses the term "global commons" to describe those areas that are not under any national jurisdiction or sovereignty and that are potentially accessible to any and all actors, be they states, non-state, or individuals. MNE 7 defines these global commons below.

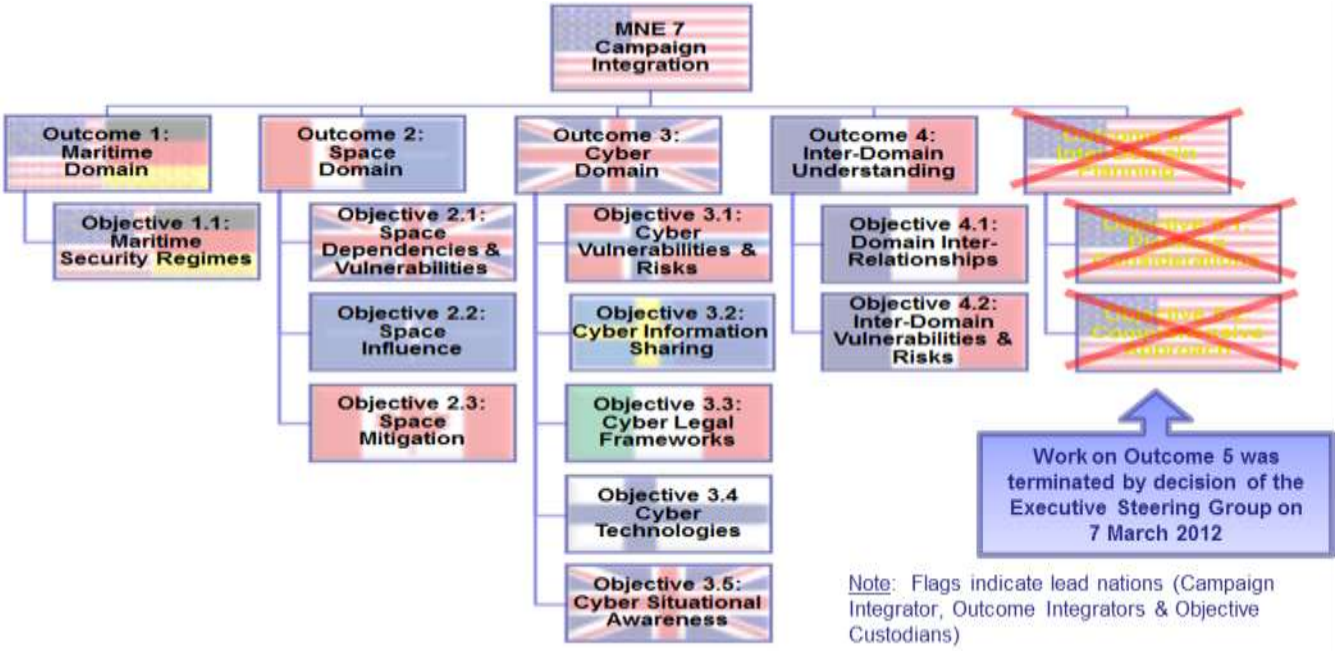
Air Domain: The global commons air domain consists of the airspace directly above the global commons maritime domain. It extends from the surface of the water to the lower boundary of the space domain.

Maritime Domain: The global commons maritime domain consists of the high seas as defined in the United Nations Convention on the Law of the Sea (UNCLOS). MNE 7 also includes in this domain other maritime areas such as exclusive economic zones and international straits which, though not part of global commons, are relevant to ensuring access to it.

Space Domain: The global commons space domain consists of the area beyond the earth's atmosphere in which no nation may claim sovereignty according to the Outer Space Treaty of 1967. The lower boundary of this area is the lowest point above the atmosphere at which an object placed in orbit does not require a constant thrust to maintain that orbit. The area has no upper boundary.

Cyber Domain: Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers.

MNE 7 was organized into four parallel lines of solution development (outcomes), each with multiple objectives, products and activities. Originally, there were five parallel lines of solution development. However, in March 2012, the fifth outcome was terminated after it was realized that it depended far more heavily than initially realized on the foundational work being done under the other MNE 7 lines of activity.



Outcome 1, **Maritime Domain**, sought to provide nations and organizations an improved ability to build or enhance maritime security regimes in order to ensure access to and freedom of action within the Maritimes Global Commons.

Outcome 2, **Space Domain**, was tasked to identify key dependencies on the space domain, identify the critical vulnerabilities of and threats to space-based capabilities, identify mechanisms to influence actors relevant to the space domain, and develop proposals for mitigation if space deterrence fails.

Outcome 3, **Cyberspace Domain**, generated solutions and products that nations and organizations can use to improve their ability to generate and sustain sufficient understanding and situational awareness of the cyberspace domain to make timely, informed and effective decisions that enables one to anticipate, deter, prevent, protect, respond, and rapidly effect an adversary's ability to disrupt or degrade one's access to and freedom of action within cyberspace.

Outcome 4, **Inter-Domain Understanding**, sought to provide analysts and planners with methodologies to arrive at a dynamic understanding of inter-domain vulnerabilities and risks that accounts for inter-domain relationships.

OUTCOME 1 (Maritime Domain)

Maritime Security Regime Cooperative Initiative

Purpose: An improved ability to build and/or enhance maritime security regimes in order to ensure access to and freedom of action within the Maritime Global Commons Domain.

Outcome Integrators

Contributors

The Maritime Domain of the Global Commons includes 139 million square miles of ocean and corridors that connect widely dispersed nations, peoples, markets and manufacturers. With 90 percent of global commerce traveling by sea and many countries relying on maritime shipping for critical energy supplies, the openness of the maritime commons is essential to a healthy international economic system, regional stability and national security. Loss of access to these global maritime highways has an adverse impact on not only regional stakeholders, but in our interconnected world it creates a ripple effect that has consequences across the globe.

The Maritime line of effort was designed to provide nations and organizations an improved ability to build and/or enhance Maritime Security Regimes (MSR) in order to ensure access to and freedom of action within the Maritime Global Commons Domain. It approached maritime access challenges through the lens of Maritime Security Regimes (MSR), which currently exist around the world in many shapes and forms and are identified through a multitude of names and titles. It should be noted that these MSRs also vary greatly in capabilities and capacities and frequently have little coordination with other MSRs.

The Maritime line of effort began by initiating case studies of existing MSRs to identify common characteristics and traits. The case studies were followed by a series of workshops, peer reviews and experiments that supported the development and evaluation of the *MSR Concept* and the *Enterprise Implementation Proposal and MSR Manual*. The findings from the experiments support the premise that a framework for the establishment of comprehensive regional and inter-regional Maritime Security Regimes, as described in the *MSR Concept* and further detailed in the *Enterprise Implementation Proposal and MSR Manual*, provide a means to better ensure access to and freedom of action within the Maritime Global Commons Domain.

For more information, please contact the MNE 7 Secretariat at mne7_secretariat@apan.org

Product 1

Regional Case Studies

These regional case studies were commissioned to methodically identify the cause-and-effect mechanisms for both successful and unsuccessful efforts of existing MSRs. The studies analyzed their respective region's politics, culture, operations, and economics, and included other assessments of the regional security orders and threats. Each study culminated with a gap analysis of the MSR's effectiveness, suggestions for their way ahead and Lessons Identified / Best Practices that could be applied to other MSRs. As such they form the baseline for the development of the *MSR Concept* and the *Enterprise Implementation Proposal and MSR Manual.*

The six MSR Regional Case Studies that were commissioned are:

- Maritime Organization of West and Central Africa (MOWCA) – led by the Combined Joint Operations from the Sea Centre of Excellence (CJOS COE)
- Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP) – led by the Combined Joint Operations from the CJOS COE
- Wider Mediterranean Region – led by Italy
- Arctic Region – led by combined efforts of Denmark and Norway.
- Gulf of Aden (GOA)/Horn of Africa – led by combined efforts of Denmark and Norway.
- Sea Surveillance Cooperation Baltic Sea (SUCBAS) – led by combined efforts of Finland and Sweden.

The Case Studies themselves will not be officially published as a MNE 7 product. However, they are available on request. Additionally, the Norwegian Institute of International Affairs (NUPI) intends to develop a working paper that further analyses communalities and differences between the MSRs. The *Manual* contains abstracts of each Case Study. The Case Studies and the Working paper could be used for further background reading personnel involved in MSR formation and enhancement.

Product 2

Maritime Security Regime Concept – "A Global Response to Regional Challenges"

MSRs often attempt to meet their regional access challenges independently without seeking assistance from other MSRs or inter-domain experts. The underlying insight of the *MSR Concept* is that the global linking of MSRs to other regions and other domains can enhance the ability of a MSR to successfully mitigate its access challenges. While a regional approach is sound, it is clear that the nature of maritime access challenges is potentially global in scope and impact.

The central idea of the *MSR Concept* is a dual approach to strengthen MSRs (1) by creating a Maritime Security Regime Cooperation Initiative, an entity that offers sustained support to encourage and facilitate collaboration between MSRs and improve their ability to access information, best practices, and expertise from beyond their own regions and (2) by implementing a program that provides procedures, principles and best practices.

The *MSR Concept* provides executive level decision makers in national governments and organizations a basis for a decision to build, join, or enhance existing MSRs. It offers a construct to improve the performance of existing MSRs and provides a framework on how to build new MSRs.

Product 3

Enterprise Implementation Proposal and Maritime Security Regime Manual

The *Enterprise Implementation Proposal and Maritime Security Regime Manual*, or *MSR Manual* for short, operationalizes the MSR Concept and describes the dual solution that (1) proposes implementing a MSR Enterprise to provide global support to regional MSRs and (2) offers processes and approaches to directly build or enhance MSR capabilities.

The *MSR Manual* consists of three parts: Part I proposes the design and required steps for the development and implementation of the MSR Enterprise while Parts II and III addresses MSR processes and capabilities required to build new MSRs and to provide sustained global enhancement of existing MSRs.

This product provides operational level personnel from existing MSRs a solid baseline how to form an MSR Enterprise. Furthermore, personnel tasked to build or enhance a MSR can use the guidance provided by the Manual to easier execute their task.

OUTCOME 2 (Space Domain)

Protecting Access to Space

Purpose: Increasing national reliance on space makes it a tempting target for adversaries, who may wish to negate economic or security advantages in other domains by disrupting space-enabled systems.

In the event of disruption or denial, protection of access to space should be improved by collaborative ability to deter/prevent disruption or denial and collaborative resilience of space capability.

Outcome Integrators

Contributors

For more information, please contact the MNE 7 Secretariat at mne7_secretariat@apan.org

Objective 2.1 – Dependencies on, Vulnerabilities of, and Threats to Space Capabilities

Most military and many civilian activities are dependent for success on support or information from space-based capabilities. There is little wide spread understanding amongst end-users of the nature and depth of their dependencies on space which are considerable and are expected to increase in the future. It was essential therefore to identify dependencies on space-based systems so that any associated risk can be managed and strategies developed. Similarly, a study into the vulnerabilities of space-based systems was necessary to determine system failure mechanisms. This work underpins the other space-related objectives.

Product

Handbook on Space Dependencies, Vulnerabilities, and Threats

The handbook is aimed at audiences working in a disparate range of military and civilian specialist and generalist areas. The approach was to create a main body of text that acted as a basic space primer, so that users can develop a simple, but sufficient, understanding of the key capabilities that space-based systems can provide. An important element of this is an understanding of: different orbits that are available; what space-based systems can do; and generic vulnerabilities of, and threats to, space-based systems.

The handbook includes ten space use-case studies ranging from Agriculture to Time Sensitive targeting. These aim to take all of the information presented in the handbook and to show how space capabilities are used.

Objective 2.2 – Mechanisms to Deter, Coerce, or Influence Space Actors

National reliance on space makes it a tempting target for adversaries, who may wish to negate economic or security advantages in other domains by disrupting space-enabled systems. Unfortunately, the combination of national dependencies on space, the cost and difficulty of protecting assets in orbit, and the environment's fragility, mean that it may be necessary to act proactively in order to protect access to space. While there are potentially a number of regulatory or financial solutions to managing actor behaviour in space, given the current absence of such mechanisms, nations will need to consider how best to deter actors from courses of action that either intentionally or unintentionally have an undesirable impact on space.

Product 1

A Process for Employing Deterrence to Influence Actors in Space

Actors in space must be motivated to pursue courses of action that do not disrupt or threaten our access to space. Overall the aim of the product is to provide a process that employs deterrence to increase the likelihood that an actor will behave in an intended manner. This product identifies how to use deterrence to manage the behaviour of actors who threaten access or use of space. It is designed in such a manner that it could be integrated with political-strategic crises management processes.

Product 2

A Deterrence Primer

The deterrence primer identifies and collates key deterrence knowledge in one place. It includes a history of the development of the typology of deterrence and describes and defines important terms. Since deterrence concerns influencing the actions of an individual or a group, the primer outlines the major theories that describe decision making as it relates to deterrence. Specifically a principal theory of the rational actor model and supporting theories that modify the ideas outlined within it.

Objective 2.3 – Space Mitigation

Space mitigation as a strategy has yet to be defined. It addresses the risk of the loss of space capability by attack or environmental hazard via cost-efficient investments in risk management to improve resiliency.

Product 1

Collaborative Space Mitigation Concept

The Collaborative Space Mitigation Concept addresses proactively the risk of the disruption or denial of key space capabilities through collaboration. Leveraging excess space capacity, partnerships, and interoperability the concept offers a potentially cost-efficient strategy for managing the risk of disruption or denial of space access. This product informs operational-level commanders and staff, national-level decision-makers, civilian bureaucrats, and industry, and could serve as the foundation for the development of national and international policies, strategies and capabilities.

Product 2

Space Mitigation Survey

A space mitigation survey was developed to review the defense community's perception of dependence on space assets and their knowledge of existing mitigation approaches in case of degradation or loss of access to the capabilities provided by these assets. The results of the survey showed that short disruptions are perceived to have moderate impact while long disruptions have extreme impacts on operations. Respondents' knowledge of mitigation measures was limited to returning to old technologies and procedures or using alternative means (e.g. high-altitude airships).

The obtained results support the view that better mitigation approaches need to be developed and that adequate training and exercises focusing on the employment of these approaches should be implemented.

Outcome 2 Overarching Product

One of the findings was the necessity of integrating the concepts of deterrence, mitigation, and resilience in order to protect access to space. To address this, the outcome developed a compact and easy to use guide, which brings together the outcome's separate products in a holistic manner and consequently highlighting their interdependencies.

Product

Guide on Protecting Access to Space

This guide draws selectively on products from the objectives as well as a 'food for thought' paper on resilience provided by the Joint Air Power Competence Center (JAPCC). Intended for use by spacefaring and non-spacefaring nations, this guide provides senior decision makers with a strategic overview of dependencies on space and options to protect access to it.

THIS PAGE INTENTIONALLY LEFT BLANK.

OUTCOME 3 (Cyber Domain)

Cyber Situational Awareness

Purpose: Decision makers can gain sufficient understanding (including legal) and situational awareness of their own networks and relevant parts of wider cyberspace, drawing upon integrated and collaborative information, improving their ability to make timely, informed and effective decisions on the actions that allow us to anticipate, deter, prevent, protect, respond and rapidly affect an adversary's ability to disrupt or degrade our access to and freedom of action within the global commons.

Outcome Integrator

Contributors

For more information, please contact the MNE 7 Secretariat at mne7_secretariat@apan.org

Objective 3.1 – Cyber Vulnerabilities and Risks

Access to and freedom of action within the cyber domain is essential for national and international security because critical networks and infrastructures are becoming increasingly dependent on it. Therefore, decision-makers must be able to identify, analyze and assess threats and vulnerabilities that may pose a risk to national and international security (e.g. critical networks and infrastructures) by disrupting or degrading access to or freedom of action within the cyber domain.

Product

Threat and Vulnerability Methodology

Objective 3.1 provides a generic and comprehensive methodology to support decision-makers in gaining a better understanding of how threats and vulnerabilities within the cyber domain can pose a risk to national and international security. This methodology highlights the dependency of critical networks and infrastructures on the cyber domain and focuses on strengthening resilience within defined areas of interest.

Objective 3.2 – Cyber Information Sharing

Access to and freedom of action within the cyber domain is essential for national security as critical networks and infrastructures are increasingly dependent on it. Therefore, decision-makers must rely on a trusted information sharing architecture that allows them to generate and maintain situational awareness within the cyber domain; increasing their confidence to take decisions and enhancing their freedom of action within the cyber domain.

Product

Information Sharing Framework

The Information Sharing Framework (ISF) provides the guidance to establish the capability to increase an organization's cyber Situational Awareness (SA) enabled by sharing information across a trusted community of interest. It describes the context and the business case for participation, and includes the collaborative governance, federated access control and management of information quality. All of which are required for effective decision making.

Objective 3.3 – Cyber Legal Frameworks

Aim to improve partners and coalition members understanding of the current international legal framework(s) applicable to the cyber domain in order to handle cyber incidents while providing decision makers with appropriate tools for decision and options for response. The Objective 3.3 community developed the following products:

Product 1

Concept Framework (CF)

An overarching framework that will enable nations to achieve an improved understanding of the current legal frameworks applicable to the cyber domain in order to assess, handle and make the appropriate response to emerging cyber incidents in accordance with the provisions of the current international law. It is anticipated that it will be used to (1) refresh national cyber strategy, (2) improve confidence in the prosecution of international cyber crimes, and (3) increase understanding of legal requirements for specific cyber issues such as attribution, territoriality, etc. (Lead Nation: Italy)

Product 2

Guidelines for Decision Makers – Legal Analysis of Cyber Incidents

This product describes how to analyze the relevant features of a given cyber incident under an international law perspective, IOT establish the violation of international rules and associate a (legally viable) set of options for response. The GDMs are meant as a supporting tool, which avoids a mechanistic approach, for the understanding of relevant legal analysis. (Lead Nation: Italy)

Product 3

Cyber Legal Lexicon

The Cyber Legal Lexicon establishes a common terminology and understanding of current legal terminology with respect to the cyber domain, based on current available sources. (Led by NATO Cooperative Cyber Defense Center of Excellence)

Product 4

Study Report on Sovereignty and Jurisdiction (SR)

This product addresses the broad topic of how contemporary IT practices align with the concepts of sovereignty and jurisdiction and current thinking in regard to the application of the concepts of jurisdiction and territoriality to the cyber domain. The NATO Cooperative Cyber Defense Center of Excellence was the lead on this study.

Objective 3.4 – Cyber Enabling Technologies

Incidents in the cyber domain may occur in a matter of seconds, potentially leading to significant adverse effects on the functionality of the victims. To protect national infrastructures and systems from cyber attacks it is necessary to understand what is happening in the cyber domain – generating and maintaining an effective situational awareness picture of the cyber environment is essential. Achieving this is dependent on sharing and displaying information from those with a dependency on the cyber domain; the span of government agencies as well as the private sector. Gaining and maintaining such situational awareness is dependent on technology for the collection, analysis, presentation and sharing of information in a relevant manner.

The main aim of this objective was to explore relevant technologies that cyber operations centers require to gain and maintain cyber SA. The challenge is that cyber SA operators do not necessarily know what to demand (what is available or possible from a technical point of view), while the technical experts do not know what cyber operators need. Hence, there is a lack of understanding related to the functional requirements for technologies as well as processes supporting situational awareness. As a result, existing technologies remain immature for effective decision-making regarding incidents in the cyber domain.

Product 1

Standard Operating Procedures for Cyber Situational Awareness

The developed standard operating procedures for a Cyber Operating Centre provide guidance on how to achieve cyber SA. It also includes functional requirements for Situational Awareness.

Product 2

Report on Current Technology to Support the Generation of Cyber SA

Objective 3.5 – Cyber Situational Awareness

There is currently a gap in our ability to gain sufficient situational awareness (SA) of the cyber domain at the national and international level. All domains have a dependency on cyberspace; cyber SA provides the underpinning confidence to carry out activities in those domains. Without a cyber SA capability the ability to put in place effective mitigation and / or resilience measures is severely reduced, leading to even greater degradation of our ability to access, and act freely within, the global commons. Nations and organizations must, therefore, collectively address an approach to generating and sustaining national and international SA of their own, and adversary activity, in the cyber domain to support their decision-making.

Objective 3.5 focuses on the situational awareness required to support decision-making in the context of cyber defense.

Product 1

Concept of Employment for Cyber Situational Awareness

A concept on how a cyber situational awareness capability can be employed; primarily written to allow the requirements for this capability to be refined by capability developers.

Product 2

Cyber Framework of Processes

A framework of processes for gaining and maintaining collaborative and integrated situational awareness of nations, or organizations, own networks and relevant parts of wider cyberspace.

Product 3

Cyber SA Limited Objective Experiment (LOE) pack

A comprehensive pack including (1) Overarching scenario and vignettes, (2) Experiment Design Solution, (3) Analysis techniques and suggested approaches, and (4) Full report and comprehensive data set from Outcome LOE.

Inter-Domain Understanding

Purpose: A dynamic understanding of inter-domain vulnerabilities and risks that accounts for domain interrelationships in order to ensure freedom of action in the global commons.

Outcome Integrator

Contributors

"Inter-domain" is the adjective qualifying something that is related to two or more different domains. For the purpose of Outcome 4, this includes the land domain as well as the Global Commons domains.

The MNE 7 Inter-Domain Understanding line of effort is divided into two inter-related objectives pertaining to the analysis of inter-domain relationships and dependencies (objective 4.1) and the determination of inter-domain vulnerabilities (objective 4.2).

Understanding inter-domain interactions is increasingly important for most engagements due, on one hand, to the level of reliance of traditional joint operations on space and cyber assets, and on the other hand, to the potential threats related to the development of anti-access and area denial capabilities in the various domains. Thus, there is a need to further understand inter-domain dependencies and the vulnerabilities that could stem from them, in the context of an operational planning process.

For more information, please contact the MNE 7 Secretariat at
mne7_secretariat@apan.org

Product 1

Methodology to Understand Inter-Domain Dependencies and Vulnerabilities

This guide is primarily intended for operational-level commanders and their staff; it is designed to support the early phase of operational planning (mission analysis and course of action development). The methodology developed in the guide complements existing intelligence, knowledge development and planning processes by providing a way to identify mission-relevant inter-domain relationships, dependencies and vulnerabilities. Its application allows a better integration of space and cyber operational issues early in the planning process.

Product 2

Pre-Doctrinal Considerations and Illustrative Examples Regarding Inter-Domain Understanding

This product seeks to raise awareness regarding inter-domain understanding and could be used for training and education purposes. It explains the importance of inter-domain understanding, proposes a conceptual framework through which to better comprehend this topic and develops generic considerations regarding the inter-domain dimension of military functions (joint functions) and related capabilities.

The illustrative examples show how the methodology could help to take into account inter-domain considerations in various types of engagements. They are based on three different engagement contexts: (1) a regional crisis where freedom of navigation in major sea lanes is at stake, (2) a situation based on the intervention in Libya in 2011 with more significant threat capabilities and (3) a humanitarian crisis implying transnational threats with significant high tech capabilities.

Inter-Domain Planning

Purpose: An ability for global commons inter-domain planning, in a comprehensive approach, to counter a disruption or denial of access to the commons.

Outcome Integrator

Contributors

Inter-domain dependencies (i.e., dependencies and influences between the air, land, maritime, space, and cyberspace domains) are increasingly important in military operations. A hazard or threat against assets or activities in one domain may deny or disrupt activities or capabilities in one or more other domains to a greater extent than envisioned previously and may, consequently, hamper military engagements as well as the normal use of Global Commons. Thus, traditional approaches to prepare and conduct operations may need to be complemented by new analysis and planning methods to better take into account inter-domain factors.

Inter-Domain Planning was designed to address two gaps identified in the Inter-Domain Baseline Assessment:

> **Inter-Domain Operational Planning**: *Nations and organizations have limited planning constructs or operational concepts that go beyond the domain-by-domain approach and fully consider the interactions between domains that characterize opportunities and challenges in the global commons.*
>
> **Inter-Domain Comprehensive Approach**: *Nations and organizations have insufficient ability to mount a comprehensive approach, which includes unified action, unity of effort and cooperation between civil and military actors across all domains of the global commons.*

The Inter-Domain Planning project was terminated in March 2012 after the AGC Executive Steering Group decided that the project depended far more heavily than initially realized on the foundational work being done under the other AGC lines of effort. However, the US project team was tasked to compile operational planning considerations that stem from the dependencies and influences between the air, land, maritime, space, and cyberspace domains based on case studies and a preliminary analysis of a typical operational environment.

For more information, please contact the MNE 7 Secretariat at mne7_secretariat@apan.org

Product

Working Draft: Pre-Doctrinal Publication on Inter-Domain Planning Considerations

This product is a compilation of planning considerations stemming from the dependencies and influences between the air, land, maritime, space, and cyberspace domains based on case studies and a preliminary analysis of a typical operational environment. Since Inter-Domain Planning was terminated in March 2012, this product is a **working draft** and is not suitable for distribution outside of the MNE 7 community.

The publication discusses inter-domain planning considerations as they relate to the Joint Functions – Command and Control; Intelligence; Fires; Movement and Maneuver; Protection; and Sustainment. The manner in which a joint force commander understands and addresses the implications of the influences and dependencies between domains in the context of the joint functions is important to the operational planner.

The case studies conducted to inform this publication include the Israeli strike against Syria and the cyberspace campaign against Estonia in 2007, the Russian campaign against Georgia in 2008, and the Stuxnet Worm in 2010.

Synthesis

Purpose: The stated mission of the Campaign Synthesis Team was to plan, coordinate and execute the synthesis effort at the campaign level. The team was formed to provide relevant insights and transitionable recommendations that supplemented the body of work accomplished by each Outcome. During Multinational Experiment 7, the working definition of synthesis at the campaign level was: The combining of different ideas, influences or objects into a new whole; by horizontally identifying insights, initiatives, and recommendations within specified focus areas that cut across and were informed by the work in multiple outcomes; in order to provide insights and recommendations to relevant agencies and organizations for further action as appropriate.

Synthesis Lead

Contributors

From a military perspective, we depend increasingly on access to the Maritime, Air, Space and Cyberspace domains – often simultaneously. The loss of access to any domain can affect our ability to operate effectively in the others. Although the four domains share many similarities, the differences between them are substantial. The goal of the campaign synthesis team was to identify themes that resonate across the domains.

The global commons might be viewed either as domains containing 'communal resources' or as domains containing 'communal spaces'. Security and military interests in the global commons concerns primarily access and therefore tend to focus on the communal spaces view; however as competition for resources becomes increasingly an underlying driver for future conflict, the communal resource view remains relevant to the military.

There are differences between alternate interpretations of the communal resources view. One view combines notions of individualism and capitalism. Under this view, benefit from the commons is shared in proportion to the investment made in extracting resources. Another view is called the common heritage of mankind. It finds that the communal resources belong to all mankind and therefore resources cannot be legally appropriated by individuals or organizations. Under the common heritage view, exploitation of the benefits of commons must be shared – irrespective of someone's participation or investment in gaining access to the resource. This difference of appreciation could be a future source of tension between users of the global commons. While this is inherently a strategic issue, given the interconnected nature of the commons, the operational commander should consider the potential impact on the joint and combined operational environment of the differing views of stakeholders.

Our militaries possess capabilities, such as situational awareness, self-defense, and independent operation, which make them unique from other agencies in their ability to operate in the global commons. These capabilities have proven utility to support our nations. Obvious examples of this are in the maritime domain, where our militaries support missions countering narcotics, piracy, proliferation, and terrorism.

In cyberspace and outer space our militaries possess similar unique capabilities that could be used. Therefore our observations relevant to this issue are:

First, there exists a body of international law (UNCLOS) that identifies to nations specific and unique duties and responsibilities for their militaries in the maritime commons. If similar law existed in cyberspace and outer space, then there would be a case for the assignment of similar duties and responsibilities, the possibility of which warrants further consideration.

Second, one of the capabilities that the military possesses that has significant utility in the global commons is situational awareness; however, domain situational awareness capabilities exist in limited quantities. This is exacerbated by national policies and cultural issues that hamper information sharing. Future work on exploiting military situational awareness capabilities in an interagency context is required and solutions that overcome policy and cultural issues need to be developed.

Third, if our militaries were called upon to provide support to law enforcement in the global commons, then military commanders will need to reconcile how to make use of information given operational intelligence requirements, which promote information for action, while supporting law enforcement needs, where information is frequently evidence. While examples of the successful management of this dilemma exist, the issue should be explored by an interagency audience addressing the cyberspace and outer space domains.

By definition, governance is limited in the global commons, in the sense that there is no identified single responsible authority. The number and types of actors in the commons are growing, as are their capabilities. Despite the fundamental differences between actors in the domains, there are a number of observations relevant to this issue:

First, today in the global commons states remain important actors, since they possess capabilities to threaten our access to the domains and they are our most significant competitors. Addressing challenges in the global commons will require a balanced assessment across states, non-states, and individuals and consideration of the threats posed by actors operating illegitimately as well as legitimate actors with whose support we can further our aims.

Second, within international relations, there are few effective mechanisms to enforce or regulate the activities of sovereign nations. States may feel disinclined to work together harmoniously and mechanisms that might force or reward states for working together do not exist or are weak.

Third, the commons are outside the sovereignty of individual states, yet by and large only states have the legal authority or responsibility to take action for breaches of law or established norms of behavior. However, failure by states to take action against, for example, piracy is commonplace. Until the situation improves, it must be accepted that breaches of both relevant law and established norms of behavior will continue, with associated consequences and risks for the users of the commons. Future work must incorporate an assumption that the laws and norms will not be universally enforced.

Fourth, the challenges of access and competition in the global commons are generally not tractable to global top-down approaches. So a more fragmented and partial approach to problem solving may be preferred, which could attract more minor players at the same time as catalyzing our nations. We can promote collaborative behavior in the global commons by choosing the nature of the problem and those involved in solving it. Collaboration on global commons issues is most successful when the issues and actors involved are local or regional, which underlines the importance of developing communities of interest.

Fifth, there exists a body of academic work that defines the global commons as areas where resources are found. While there are fundamental differences between the resource and the communal spaces views, there are sufficient analogous issues to believe that academic work might be relevant to parts of the military problem. Academia has developed a language to describe the commons and identified characteristics of successful regimes for governance and management. This body of work could be exploited more comprehensively when considering the global commons.

Finally, in the global commons opponents will likely use international law or rules of engagement as a force multiplier to traditional military means. This could manifest itself as public interpretation of law to intentionally impede our access to the commons or it might be the use of an asymmetrical approach, where opponents exploit our known adherence to law or self-imposed constraints in rules of engagement. Coordination to develop common approaches could be further exploited to deter or mitigate this challenge.

THIS PAGE INTENTIONALLY LEFT BLANK.

Impact of the Multinational Experiment Series

The Multinational Experiment (MNE) series was designed to develop and validate concepts and capabilities that can be used to address the challenges associated with conducting coalition operations. To date, seven experimentation campaigns have been conducted in this series under the themes of **collaboration**, **effects-based operations**, **comprehensive approach**, and **access to the Global Commons**.

COLLABORATION	
	**Multinational Limited Objective Experiment (LOE) 1,** Technical Distributed Collaboration (South Pacific Vignettes), November 2001, investigated coalition military planning in a combined joint task force within a distributed, multinational collaborative information environment.
	**Multinational LOE 2,** Multinational Information Sharing (Pacific Rim Vignettes), February 2003, studied development of coalition operational net assessment (ONA), which encompasses a product, process, and organization focused on developing detailed understanding of operational environment, as well as effects of friendly and adversarial actions in battlespace.
EFFECTS BASED OPERATIONS	
	**Multinational Experiment 3,** Effects-Based Planning (Afghanistan Scenario), February 2004, examined issues associated with Coalition Interagency Coordination Group(s); Intelligence, Surveillance and Reconnaissance (ISR); multinational information sharing; logistics; coalition-based health services support; information operations; and knowledge management.
	**Multinational Experiment 4,** Effects-Based Approach to Operations (Afghanistan Scenario), February – March 2006, explored how DIME elements of effects-based approach to operations (EBAO) affect behavior of adversaries. It also examined multinational interagency group coordination, multinational logistics interoperability, information operations, and medical support.
COMPREHENSIVE APPROACH	
	**Multinational Experiment 5,** Comprehensive Approach (African Scenario), May 2006 – December 2008, explored a multinational, interagency, comprehensive engagement strategy to influence a stable international environment; sought to broaden the context of pre-crisis and crisis management by engaging both military and non-military interagency organizations.
	**Multinational Experiment 6,** Countering Irregular Threats with the Comprehensive Approach, June 2008 – December 2010, developed improved coalition capabilities to counter activities of irregular adversaries and other non-compliant actors while supporting a Comprehensive Approach.
ACCESS TO THE GLOBAL COMMONS	
	**Multinational Experiment 7,** Access to the Global Commons, January 2011 – December 2012, developed concepts and capabilities to anticipate, deter, prevent, protect against, and respond to a disruption or a denial of access to the global commons domains and for ensuring freedom of action within them, while taking into account their interrelationships.

Participation in the MNE series has allowed partners to develop national Concept Development and Experimentation (CD&E) capabilities while collaborating on shared problems. In addition, participating nations and organizations have used the MNE campaigns to supplement national-level efforts to improve how joint and coalition operations are conducted and inform their national strategies, doctrines, and operating procedures.

- The Multinational Limited Objective Experiments and early MNE campaigns contributed to the development and implementation of the Joint Semi-Automated Forces (JSAF) modeling and simulation application and the development of the Coalition Federated Battle Lab Network (CFBL Net). These resources are used to support distributed training and capability development with the U.S., NATO, and multinational communities.

- Multinational Limited Objective Experiment 1 significantly influenced the United States Joint Forces Command's (USJFCOM) work on Rapid Decisive Operations planning and the Multinational Interoperability Council's (MIC) effort to develop a Lead Nation concept for planning and execution of coalition operations.

- Multinational Limited Objective Experiment 2 significantly influenced USJFCOM's development of the Standing Joint Force Headquarters (SJFHQ) concept and informed important work on Operational Net Assessment (ONA) and the Multinational Information Sharing (MNIS) Concept of Operations (CONOPS) within USJFCOM, the NATO Concept Development and Experimentation (CD&E) Working Group, and the MIC.

- Multinational Experiment 3 influenced and informed U.S., NATO and MIC work on the following coalition warfighting concepts: SJFHQ; Effects-Based Planning, Effects-Based Operations (EBO); ONA; Collaborative Information Environment; Coalition Interagency Coordination Group; Joint Intelligence, Surveillance, and Reconnaissance (ISR); and MNIS. They also significantly informed the development of the initial CONOPS and organizational architectures for the NATO Response Force (NRF).

- Multinational Experiment 4 influenced U.S. and NATO work on the following coalition warfighting concepts: EBO, Effects Tasking Order, Knowledge Base Development (KD), Knowledge Management, Information Operations (Info Ops), Multinational Interagency Coordination Group, and MNIS. They also directly supported development of a pre-doctrinal Effects Based Approach to Operations Handbook for the NRF.

- Multinational Experiment 5 influenced and informed coalition-wide work on warfighting concepts related to Multinational Interagency Strategic Planning, Cooperative Implementation Planning, and Cooperative Management and Evaluation. They also directly supported development of NATO's Comprehensive Operations Planning Directive and improvement and expansion of its Tool for Operational Planning, Force Activation and Simulation (TOPFAS).

  The work under MNE 3, 4, and 5 also informed the *European Union Concept for Military Information Operations*, 25 February 2008.

- Multinational Experiment 6 significantly influenced coalition-wide development of warfighting concepts related to Security Implementation and Transition, Strategic

Communication, Campaign Assessment, and Shared Situational Awareness. It also directly supported writing of the NATO Knowledge Development handbook, further improvement of TOPFAS, development of the NATO Maritime Situational Awareness package, and revision of U.S. Army Field Manual 5-0 (The Operations Process). Perhaps most significantly, MNE 6 led to production of doctrinal guidelines for security transitions that were adopted directly by Headquarters, International Security Assistance Force (ISAF) and development and direct fielding of an automated tool to allow all ISAF partners to gain and maintain theater-wide logistics situational awareness.

The work on the Comprehensive Approach during MNE 5 and 6 formed the basis of Austrian national security doctrine informed lectures within Austrian Joint Command and General Staff Courses and Austrian Military Leadership Courses. In addition, the MNE 5 and 6 informed the MIC's *Comprehensive Approach Framework – A Military Perspective*, 07 June 2011.

MNE 6 produced a set of products that dealt with Cultural Awareness. Noteworthy among the products, the Cross-Cultural Awareness concept, the anthropological study of Afghanistan, and a suite of training materials that have been used in Afghan-theater pre-deployment training for the Spanish Army units.

During MNE 6, Spain and Finland developed the Multinational Interagency Situational Awareness-Extended Maritime Environment (MISA-EM) conceptual framework that added situational awareness to a maritime operations center. Based on this framework and its associated tool requirements, the Spanish Navy designed a plan for engaging with national and international stakeholders in the maritime realm and developed the "AQUA" portal – a collaborative tool that allows information sharing among trusted agents from stakeholder organizations. The Baltic Sea region nations have also implemented MISA-EM products and concepts within the Surveillance Co-operation Finland-Sweden (SUCFIS) and Sea Surveillance Co-Operation Baltic Sea (SCUBAS) constructs.

- A sampling of NATO documents that have been informed by various MNE campaigns is given below:
    - *ACO Comprehensive Operations Planning Directive (COPD) – Interim*, 17 December 2010 (from MNE 3/4/5/6)
    - *AJP-3.10 – Allied Joint Doctrine for Information Operations*, 23 November 2009 (from MNE 3/4/5)
    - *Bi-SC Pre-Doctrinal Effects-Based Approach to Operations (EBAO) Handbook*, 04 December 2007 (from MNE 3/4)
    - *Bi-SC Pre-Doctrinal Knowledge Development (KD) Handbook*, 09 February 2011 (from MNE 3/4/5/6)
    - *Lisbon Summit Declaration – NATO's Commitment to a Comprehensive Approach*, 20 November 2010 (from MNE 5)
    - *MC 422/3 – NATO Military Policy on Information Operations*, 08 July 2008 (from MNE 3/4/5)
    - *Strategic Communications Military Capability Implementation Plan*, 20 June 2011 (from MNE 6)
- Finland and Austria are already reaping the benefits of the cyber work conducted under Multinational Experiment 7. Finland's National Cyber Security Strategy

benefits from MNE 7 Cyber Outcome products and studies, especially the MNE 7 work conducted on integrated cyber situational awareness and on the cyber legal concept framework. For Finland, the standard operating procedures developed for cyber security centers will be implemented or further developed in future work. Similarly, MNE 7 work is an input into the Austrian National Cyber Strategy and into the Austrian military Computer Emergency Response Team (milCERT).

It is also anticipated that MNE 7's work on maritime security regimes (MSR) will significantly inform existing MSRs and will improve collaboration between MSRs.

THIS PAGE INTENTIONALLY LEFT BLANK.